AOS-W 3.4.2.6

Release Notes

This document describes new features and issues pertinent to the AOS-W 3.4.2.6 release.

What's New in This Release

AOS-W 3.4.2.6 is a patch release that addresses and provides solutions to a number of known issues.

For details on all of the features described in the following sections, see the *AOS-W 3.4.2 User Guide*, *AOS-W 3.4.2 CLI Reference Guide*, and *AOS-W 3.4.2 MIB Reference Guide*.

NOTE

See the *AOS-W 3.4.2 Software Upgrade Guide* for instructions on how to upgrade your switch to this release.

In Previous AOS-W 3.4.2 Releases

Previous releases of AOS-W 3.4.2 have introduced new software features for all Alcatel-Lucent switches. This section describes new features and capabilities of AOS-W 3.4.2.

Multicast Traffic Optimization

The command is added in AOS-W 3.4.2.5 (bug 42278)

A new command is added to support further enhancement to the Controller's Dynamic Multicast Optimization feature. The command is:

```
(config) #firewall shape-mcast
```

Broadcast and Multicast Traffic Optimization

This feature is added in AOS-W 3.4.2.5 (bug 42132) and replaces

Broadcast and Multicast traffic from APs, remote APs, or distributions terminating on the same VLAN floods all VLAN member ports. This causes critical bandwidth wastage especially when the APs are connected to L3 cloud (where available bandwidth is limited or expensive). Suppressing VLAN BCMC traffic to prevent flooding can result in loss of client connectivity.

To effectively prevent flooding of BCMC traffic on all VLAN member ports, use the **`bcmc-optimization`** parameter under the `interface vlan` command. This parameter ensures controlled flooding without compromising client connectivity. By default this option is disabled. You must enable this parameter for the controlled flooding of BCMC traffic.

NOTE

The **`bcmc-optimization`** parameter replaces the **`ip-local-proxy-arp`** parameter under the **`interface vlan`** command.

When the bcmc-optimization parameter is enabled, the controller sends the wireless client MAC address, in response to an ARP request, if the wireless client is in the association table.

The **bcmc-optimization** parameter has the following exemptions:

- All DHCP traffic will continue to flood VLAN member ports even if the **bcmc-optimization** parameter is enabled.
- The switch will do proxy ARP if the target IP entry exists on the switch. If the target IP does not exist on the switch, ARP requests will be flooded on all VLAN member ports.

You can configure BCMC optimization in CLI and in the WebUI.

In the CLI

```
(host) (config) #interface vlan 1
(host) (config-subif)#bcmc-optimization
(host) (config-subif)#show interface vlan 1

VLAN1 is up line protocol is up
Hardware is CPU Interface, Interface address is 00:0B:86:61:5B:98 (bia
00:0B:86:61:5B:98)
Description: 802.1Q VLAN
Internet address is 10.17.22.1  255.255.255.0
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled, BCMC Optimization enable
Encapsulation 802, loopback not set
MTU 1500 bytes
Last clearing of "show interface" counters 12 day 1 hr 4 min 12 sec
link status last changed 12 day 1 hr 2 min 21 sec
Proxy Arp is disabled for the Interface
```

In the WebUI

1. Navigate to **Configuration** > **Network** > **IP**.
2. In the **IP Interfaces** tab, click the **Edit** button of the VLAN for configuring BCMC optimization.
3. Select **Enable BCMC** check box to enable BCMC Optimization for the selected VLAN.

EIRP Maximum Cap Includes Support for Cisco Telephones

This release of AOS-W includes new parameters in the 802.11a and 802.11g radio profiles that support a workaround for a known issue on Cisco 7921G telephones. When you use these parameters to specify a cap for an radio's maximum equivalent isotropic radiated power (EIRP), even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons. This feature is disabled by default.

To set a capped EIRP via the command-line interface, use the following commands, where <*cap-reg-eirp*> is the capped maximum EIRP in dBm. The supported range is 1–31 dBm.

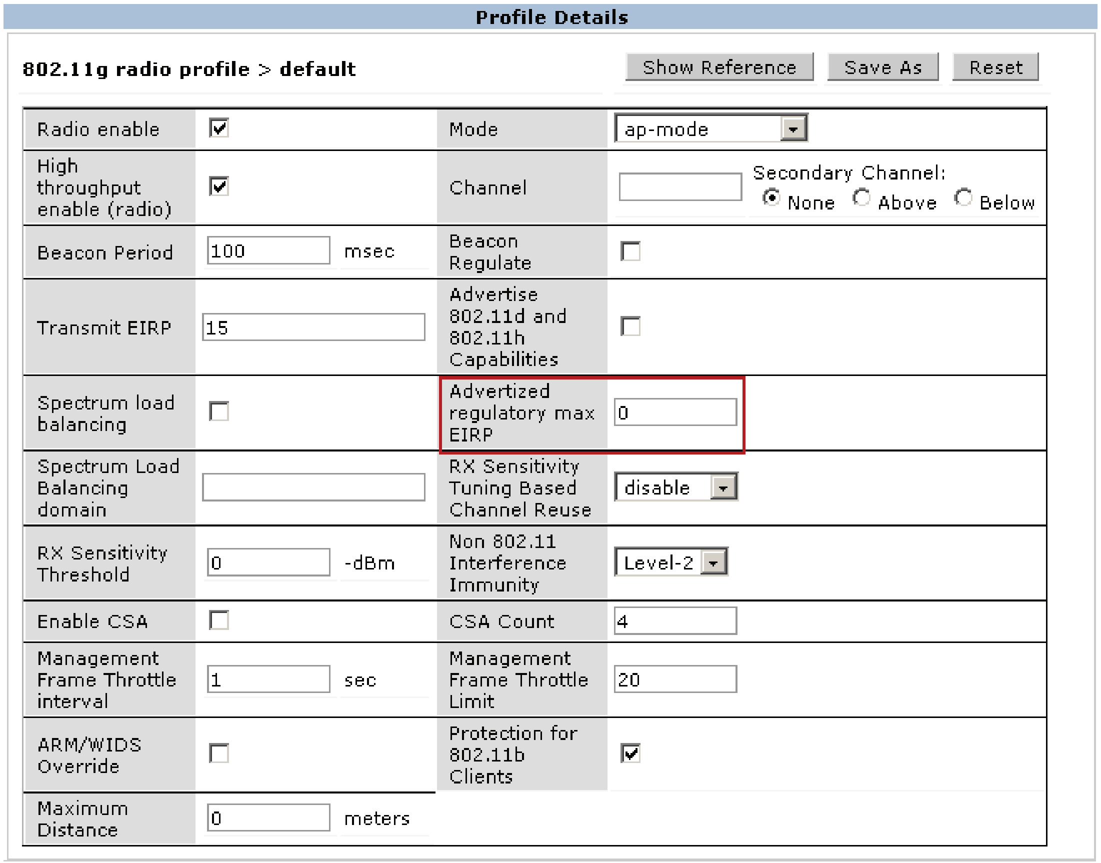
```
(host)(config) #rf dot11a-radio-profile default cap-reg-eirp <cap-reg-eirp>

(host)(config) #rf dot11g-radio-profile default cap-reg-eirp <cap-reg-eirp>
```

To configure this parameter via the WebUI:

1. Navigate to **configuration>All Profiles**.
2. In the Profiles list, expand the **RF** menu, and select either **802.11a radio profile** or **802.11g radio profile**.
3. In the **Profile Details** window, select the profile for which you want to configure an advertised regulatory maximum EIRP level.

4. In the **Advertised regulatory max EIRP** field, enter the maximum power level to be advertised by any radios using that profile, in dBm. The supported range of values is 1–31, and the default value is 0, which disables this feature.
5. Click **Apply** to save your changes.

Figure 1 *Configuring an Advertised Regulatory Max EIRP via the WebUI*



Profile Details

802.11g radio profile > default

Radio enable	☑	Mode	ap-mode
High throughput enable (radio)	☑	Channel	Secondary Channel: ● None ○ Above ○ Below
Beacon Period	100 msec	Beacon Regulate	☐
Transmit EIRP	15	Advertise 802.11d and 802.11h Capabilities	☐
Spectrum load balancing	☐	Advertized regulatory max EIRP	0
Spectrum Load Balancing domain		RX Sensitivity Tuning Based Channel Reuse	disable
RX Sensitivity Threshold	0 -dBm	Non 802.11 Interference Immunity	Level-2
Enable CSA	☐	CSA Count	4
Management Frame Throttle interval	1 sec	Management Frame Throttle Limit	20
ARM/WIDS Override	☐	Protection for 802.11b Clients	☑
Maximum Distance	0 meters		

Kerberos Authentication

AOS-W now supports Kerberos authentication. This feature can only be configured through the CLI and includes the following new CLI commands:

- `(host) (config) #aaa authentication stateful-kerberos <profile-name>`
- `(host) (config-role) #stateful-kerberos <profile-name>`

To enable Kerberos authentication, open the CLI on your switch and complete the following steps:

1. Create a Windows server

```
(host) (config) #aaa authentication-server windows <server-name>
(host) (Windows Server "<server-name>") #host <ip-addr>
(host) (Windows Server "<server-name>") #enable
```

2. Create a server-group and assign the windows server to this group

```
(host) (config) #aaa server-group <server-group-name>
(host) (Server Group "<server-group-name>") #auth-server <server-name>
```

3. Create a Kerberos authentication profile. Then associate the server-group and default Kerberos-authentication successful role

```
(host) (config) #aaa authentication stateful-kerberos <profile-name>
(host) (Stateful Kerberos Authentication Profile "<profile-name>") #server-group
<server-group-name>
(host) (Stateful Kerberos Authentication Profile "<profile-name>") #default-role
authenticated
```

4. Link the Kerberos profile to a user-role

```
(host) (config) #user-role <user-role>
(host) (config-role) #stateful-kerberos <profile-name>
```

Management Password Policy

By default, the password for a management user has no requirements other than a minimum length of 6 alphanumeric or special characters. However, if your company enforces a best practices password policy for management users with root access to network equipment, you may want to configure a password policy that sets requirements for management user passwords.

The new Password Management Policy profile can be configured to require a specified number of letters, numbers and special characters in a management user's password, put limits on the number of repeating characters in the password, and set the number of failed management user login attempts that will result in the management user being locked out of the network for a period of time.

Memory Monitor Enhancement

Memory monitor now saves 30 snapshots of detailed memory debugging information. There are no longer any minimum memory requirements and the logs rotate to keep the freshest ones first.

These reports provide information on system memory, irregular application memory usage, large files in the ramdisk, large pending tx/rx queues, and memory blocks usage. This information will be leveraged for tech support logs and nanny post-crash reports.

Beacon Regulation

This change was added as a solution to Bug #35825.

Enabling this setting introduces randomness in the generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. To enable this though the CLI:

```
<host> (config) #rf dot11a-radio-profile <profile-name> beacon-regulate
<host> (config) #rf dot11g-radio-profile <profile-name> beacon-regulate
```

To enable this through the WebUI, navigate to **Configuration > Advanced Services > RF Management > 802.11a** or **802.11g Radio Profile > <profile name>**. Check the **Beacon Regulate** check box to enable this feature.

New CLI Commands

The following commands have been added in the AOS-W 3.4.2 Command Line Interface.

Table 1 *New CLI Commands for AOS-W 3.4.2*

Command	Description
`aaa password-policy mgmt`	Define a policy for creating management user passwords.
`show aaa password-policy mgmt`	Show the current password policy for management users.
`show memory debug [verbose]`	Display detailed memory information to debug memory errors the switch. This command should only be used under the supervision of Alcatel-Lucent Technical Support.

Issues and Limitations Fixed in AOS-W 3.4.2.6

This release contains all fixes up to and including those in AOS-W 3.4.2.0. The following issues and limitations have been fixed in the AOS-W 3.4.2.6 release:

Fixed in AOS-W 3.4.2.6

Table 2 *Fixed in AOS-W 3.4.2.6*

Bug ID	Description
42132	When `ip local-proxy-arp` on `interface vlan` is enabled, ARP for wireless clients are no longer broadcasted to all APs that share the same user VLAN. Instead switch does proxy-arp for the wireless client.
42728	An issue in which APs rebootstrapped, with the message "Rebootstrap requested by STM," when Mode Aware is enabled has been fixed. The problem is caused by multiple changes between forwarding modes, creating inconsistencies.
43236	Continuous, unexpected AP reboots caused by a problem in the SAPD process has been fixed.
43375	The switch no longer does proxy-arp requests between wired clients, when local-proxy-arp is enabled, when both the destination and source clients are reachable on the same interface as the switch.

Fixed in AOS-W 3.4.2.5

Table 3 *Fixed in AOS-W 3.4.2.5*

Bug ID	Description
28966, 34015	The command `show ap association` now displays the correct tx and rx datarate values.
35308	Additional files for analyzing an HTTPD core dump will be collected and will be included in the file generated by the tar crash command.
36386	Mesh points correctly support the Taiwan regulatory domain (TW) on a switch with configured with the Taiwan country code.
36679	Changes to datapath timers increases switch stability.
37899	Improved OSPF route table calculations prevent a timeout which can cause APs to rebootstrap.
38401	The **Security>Authentication> Servers** window in the AOS-W WebUI can display up to 100 user entries at a time.
38410	The output of the `show inventory` command displays the correct line card values.
38626	A switch processor exception due to a segmentation fault on the WMS module has been fixed.

39604	File names cannot be created, exported, or imported with any of the following special characters:
	~@#$%^&*()+={}[]<>/\\\|
	This restriction applies to the following CLI commands:
	`wms export-db`
	`wms export-class`
	`local-userdb export`
	`local-userdb import`

39656	The output of the `show inventory` command displays the correct power supply values.

Table 3 *Fixed in AOS-W 3.4.2.5*

Bug ID	Description
39842	A log file is created when mode-aware ARM converts an AP to an Air Monitor or an Air Monitor to an AP. This information can be seen via the command `show log wireless`.
40174	Changes to datapath timers increases switch stability.
40246, 40351	The issue with OAW-AP124 configured as a mesh point and connected to a switch with country code DE or JP taking long time to reboot has been fixed.
40270	The issue with switch rebooting due to low free memory has been fixed.
40346	The issue with remote APs performing panic reboot on receiving more than 4K ACE has been fixed. The remote APs are now set to handle upto 8k ACE entries.
40554	Users can now poll the `wlsxSwitchUserTable` MIB to view the list of users connected to a switch.
40917, 41724	When ACLs with large number of ACE entries (over 600) were pushed to a remote AP over a slow network link, the remote AP did not successfully receive the ACLs. This issue has been fixed.
40942, 41813, 41819	The DBSYNC code was updated to prevent a number of issues including the switch running out of memory when queuing files for send, re-entrant PAPI ACKs corrupting the largePapi buffer, and simplifying the state of the switch in general.
41094	The command `show references user-role <user-role-name>` now correctly displays the profiles in which the queried user-role has been configured.
41221	SNMP agent timeouts are displayed as errors in the error log.
41228	The issue with unreachable ESI servers not being removed from an ESI group has been fixed.
41255, 37033, 37376, 37922, 38805, 42278	Multicast streaming video performance is improved.
41769	Idle timeout for IPv6 users is now supported on 6000 Series, 4X04 Series, and 4306 Series switches.
42012, 34041	The issue with APs rebooting continuously after upgrade to 3.4.2.3 has been fixed.
42126, 41913, 36281	The issue with multicast traffic flooding all APs (with IGMP snooping enabled) has been fixed.
42132	The local-proxy-arp feature now sends the ARP response on behalf of the client with switch MAC address and does not flood all APs with ARP broadcast requests. Use the `bcmc-optimization` command for the appropriate VLAN to prevent flooding of broadcast-multicast traffic.

Fixed in AOS-W 3.4.2.4

Table 4 *Fixed in ArubaOS 3.4.2.4*

Bug ID	Description
39153	The WebUI will be able to display the SSID info for Alcatel-Lucent virtual APs even if the 'hide-ssid' has been enabled for that virtual AP.
39737	Memory is now correctly freed after the client sends a deauth and dissociates from the AP.
39997	Running the s**how ap debug system-status** CLI command repeatedly no longer causes memory errors on the AP.
40831	The internal tunnel cleanup timer interval has been increased to prevent rare instances of premature cleanup of packets that stay in queue of the security engine for longer time than expected.

Fixed in AOS-W 3.4.2.3

Table 5 *Fixed in AOS-W 3.4.2.3*

Bug ID	Description
34143	Alcatel-Lucent OAW-S3 model switches have improved IP routing behavior for L3 VLANs.
34299, 36277, 38701	Voice ALG is now correctly notified when session is deleted based on a user ageout.
34560	An AP will ignore Aeroscout RTLS magic cookie, until the AP is configured to strem to the Aeroscout RTLS server.
35459	A CLI command has been added that allows the user to remove DHCP option 43 from the config file if needed. This option is part of the default configuration. To remove this option use: `(config-dhcp) #no vendor-class-identifier`
35518, 39757	The error message “Error Uploading Certificate: CertMgr error” no longer appears in the WebUI when the certificate has been successfully uploaded.
35939	When an S3 is removed from a chasis while in operation, the switch will no longer reboot. Instead, the following critical message is displayed in the syslog: `Communication with the Peer S3 in the Bottom slots is broken. Please check the Bottom slot to make sure it is operational`
36921	The “1000” LED on ports 1/4 and 1/5 on the OmniAccess 4306G now works correctly.
36999	Improvements to 802.1x wired termination with MUX and Secure Jack prevents the switch from sending an EAP packet to the backend server if EAP termination is enabled on switch.
37234	Alcatel-Lucent 11n APs Tx rate is 300 Mbps.
37500	Taking a flash backup from the WebUI no longer causes the switch to reboot due to low memory.
37753	When the VRRP state changes, the change is logged at the WARNING level in the syslog.
37842	Switches now correctly accept 802.1Q frames with null VLAN IDs on access ports.
38348	An IP reassembly failure in the MUX server’s datapath, which prevented the download of logon scripts when upgrading AOS-W, has been fixed.

Table 5 *Fixed in AOS-W 3.4.2.3*

Bug ID	Description
38447	Mobility will not interrupt a client's new DHCP cycle by de-authing the associated station.
38500	If a client roams to a virtual AP where mobility is disabled, DHCP relay agent now uses the new VLAN IP for requests.
38584, 39551	A DNSMASQ crash has been fixed by excluding DNSMASQ from nanny monitoring on XLR platforms.
38628, 39396	A switch process exception caused by a segmentation fault in the SNMPD module has been fixed.
38663	Connectivity issues caused when a local switch sees another local switch's APs as interfering, while WMS-offload is enabled via an AMP, have been fixed.
38705, 30366	An auth crash caused when a long username and long password (longer than 250 characters) are entered into the Captive Portal login screen has been fixed.
38789, 39021	APs properly respond to 802.11 authorization requests from a Dell wireless NIC in non-DFS channels.
38898	A number of improvements have been made to AM-mode APs to reduce their steady-state overhead.
38900	Gateway health checks can now be enabled from configuration mode in the CLI.
38995	An unexpected switch reboot caused by an error in the fpapps process has been fixed.
39100	Call status is cleared when SIP is aged out from the user table.
39299	An snmpd process malfunction caused by a memory corruption has been fixed.
39339	XML API user_delete now works correctly, even if the MAC address tag is not set.
39426, 39988, 40422	An unexpected STM module crash has been fixed.
39431, 33382, 36869, 36218, 39779	Heat maps no longer appear randomly grabled in the WebUI.
39444	The auth module on the switch has been improved to increase switch stability and reduce unscheduled switch reboots.
39525	Captive portal DNS intercept now works correctly with users connected to an untrusted VLAN.
39563	All policy rules are now correctly displayed in the WebUI.
39615	A trapd-module process crash on a OAW-S-2switch has been fixed.
39676	This version of ArubaOS has been updated to work around an issue on Cisco 7921G phone transmission power, where Cisco phones can erroneously mask the 6th bit of an AP radio's advertised maximum EIRP. This new parameter ensures that these Cisco phones will continue to transmit at a desired power level. For details, see "EIRP Maximum Cap Includes Support for Cisco Telephones" on page 1.

Table 5 *Fixed in AOS-W 3.4.2.3*

Bug ID	Description
39737, 40985	Memory is now correctly freed after the client sends a deauth and dissociates from the AP.
39784, 39290	IPv6 packets no longer become corrupted after passing throught a 4306 Series or 4X04 Series switch when IPv6 firewall is enabled.
39912	User will now be locked out of the WebUI, after exceeding the number of failed login attempts, based on the configured time, not just 3 minutes.
39924, 39601	Roaming performance during a love OCS audio/video call is no longer adversely affected by the “classify-media” feature is enabled on the user ACL.
40033	OID values are no longer lost when upgrading to 3.3.3.x.
40065	Extraneous bytes are no longer added to tagged or untagged traffic that passes through 4306 Series switches.
40145	Memory enhancements improved the login process for captive portal authentication.
40181	The DHCP timeout for a transaction ID has been increased on all AP platforms.
40315, 34967, 37402	An issue in which APs failed to come back up after configuration has been fixed.
40599	An auth module crash, whihc caused a number of APs to become inactive, has been fixed.

Fixed in AOS-W 3.4.2.2

Table 6 *Fixed in AOS-W 3.4.2.2*

Bug ID	Description
39977	A kernal panic which occured regularly on the 4306GW when sending traffic to a wireless client has been fixed.
	This patch also includes fixes for some issues found internally.

Fixed in AOS-W 3.4.2.1

Table 7 *Fixed in AOS-W 3.4.2.1*

Bug ID	Description
35125, 35166, 35427, 35717, 35936, 35973, 36337, 36550, 36594, 36336, 36503, 37009, 37087, 37131, 37272, 37285, 37377, 37398, 36872, 37518, 37839, 38242, 38278, 38312, 38540, 38564, 38683, 38769, 36844, 39045, 39178	Unexpected switch behavior caused by a Control Process Kernal Panic has been fixed.
35285	Idle wireless VPN users are no longer deleted from the auth table when ICMP response from the inner IP address is returned on a different ingress tunnel.
35727	PMK cache memory leak is fixed.
35858, 38929	Imported campus entires will be successfully merged into the backup flash database after a switch reboot.
36652, 36960	Unexpected switch behavior caused by a datapath exception has been fixed.
36653, 38937	PMK caching for EAP-LEAP authentication has been fixed, allowing roaming clients to fall into the correct role when moving from one switch to another.
36746	Descriptions of the 10GB ports added in the CLI are preserved across reboots.
36810	When using XML-API, passwords may have trailing spaces.
36901, 37420, 37457, 37497, 37534, 37917, 38467, 38774, 37190	This build has resolved multiple memory errors that may cause the switch to stop responding or reboot.

Table 7 *Fixed in AOS-W 3.4.2.1*

Bug ID	Description
37027	VRRP flapping, which results in AP bootstrapping when running `show inventory` has been fixed.
37247	An auth module crash caused by an inconsistency of the ACE table between auth and datapath has been fixed.
37250, 37260	An issue in which STM is unable process messages from connected APs, resulting in the APs never coming up and continually rebooting, has been fixed.
37565	An issue in which migrating WMS to an AMP caused local switches to lose free memory has been fixed.
37643	An auth process crash caused by user entries cached in a local db tied to a VPN user role that no longer existed on the switch has been fixed.
37783, 39164	The default ap-inactivity-time has been increased to 20 sec. This reduces the message flow to WMS on master due to discovery of APs with low RSSI by AM or by an AP on its home channel. Additionally, the mysql query that retrieves the probe MAC address for a station has been optimized. The new scan will prevent the full table scan from being done. The rows retrieved by mysql will be a lot smaller when compared to a full table scan being done in the old query.
38073	SSLCipher settings of web server have been modified such that LOW, MEDIUM and HIGH cipher aliases are cumulative. LOW=LOW+MEDIUM+HIGH, MEDIUM=MEDIUM+HIGH and HIGH=HIGH. This allows webserver to allow strongest SSL cipher according to configuration settings.
38130	A switch crash due to the UDB server module error has been fixed.
38177	Spanning Tree Protocol can now be enabled at the port level through the WebUI.
38180	An auth crash caused by a username with long leading spaces, which overruns the buffer, has been fixed. AOS-W now properly handles oversized usernames.
38186, 39354	VPN authentication now works correctly with Windows 7 clients.
38216, 38334	Radio TX queue statistics will now sync upon radio reset, which will prevent any unusual statistics issues that result in false nanny initiated external resets.
38239, 39239, 39390, 39391	A switch reboot issue cause by a datapath timeout has been fixed by increasingthe number of station list entries and reduced the number of stations per list to decrease memory footprint.
38250	An issue in which a time range incorrectly being inserted into User Derivation rules, and remians after deletion, has been fixed.
38283, 38620	An STM crash caused by a stack overflow, which resulted in AP bootstrapping, has been fixed.
38453	A fix has been added to prevent VRRP from starting before fpapps to prevent a standby switch from transitioning to a master state upon reboot.
38523	Unexpected switch behavior caused by an STM module crash has been fixed.
38569	Guest provisioning policy text is now properly displayed when it contains Japanese characters.
38644	The BR (Brazil) regulatory domain now shows all the allowed indoor and outdoor channels.

Table 7 *Fixed in AOS-W 3.4.2.1*

Bug ID	Description
38659	An auth memory leak caused by RADIUS timeouts has been fixed.
38661	Memory leak related to Auth timers is now fixed.
38697	Throughput fluctuations caused when frames are sent out of sequence, causing confusion on the receiver' block ACK window, has been fixed.
38727	An AM crash that occurs during a packet capture when data frames exceed the maximum buffer size has been fixed.
38951	Support for the country code SA on the OAW-AP105 has been enabled.
39784, 39290	IPv6 packets no longer become corrupted when passing through 4306 or 4x04 Series switches.

Fixed in AOS-W 3.4.2.0

Table 8 *Fixed Issues in AOS-W 3.4.2*

Bug ID	Description
27841, 38261	New ports added under the Port-channel interface now show up correctly in `show running-config`.
31288	The LINK/ACT LEDs for ports 1/6 and 1/7 on the 4306 series switch now work correctly.
34298, 35703	Bi-directional voice sessions do not age out when activity is present on only one direction.
35349	The AP Status LED on the front of switches now work correctly.
35485	A new backup config file is not created in the flash everytime the switch is reloaded.
35926	For the OAW-AP120 series, the MAX RTS retries for a single data frame has been changed to 6. Additionally, the AP will not try to resend the frame, instead sending the next frame.
35927, 36846, 35910	Stateful firewall netdestination now allows any subnet mask to be entered in the WebUI.
35937, 35942, 35946, 35943, 35945	When downgrading from 3.4.2.0 to a pre-3.4 build, the local user database can be successfully imported using the file called `legacy_db.udb`. This file is generated when the switch is upgraded to 3.4.2.

36212,
38287
	When the system clock is changed on a switch, the following warning message is displayed to inform the user that the switch must reboot:
	`WARNING: Changing the system clock will require a reboot of the switch.`
	This message is followed by another message asking the user:
	`Are you sure you want to continue(y/n): y`
	`Switch Real Time Clock is changed. The switch must be rebooted now.`

36327, 36723	An fpcli memory leak has been fixed.

Table 8 *Fixed Issues in AOS-W 3.4.2*

Bug ID	Description
36789, 36060	Community read strings, name, and location are correctly displayed in the WebUI after being entered there.
37012	Manual clock changes are now logged in the audit trail.
37172	An issue in which RAPs did not come up after upgrading has been fixed.
37215	The uplink manager on 4306 Series switches is now disabled by default.
37281	The default values for handoff-assist have been changed to: ● rssi-falloff-wait-time = 4 seconds ● low-rssi-threshold = 20 ● rssi-check-frequency = 3 seconds
37301	Fan status is now correctly displayed in the show inventory output for an SC-1.
37315	The switch, license, and WLAN wizards now display correctly and do not show a blank page.
37405	VLAN 4094 is no longer allowed to be created on an M3, but is still allowed on other platforms.
37430, 37910	If both EAP-types are configured, then TLS is now attempted before PEAP.
37456	Unexpected switch behavior caused by a datapath exception has been fixed.
37494, 38472	An issue in which an OAW-AP125 crashes when configured with a persistent SSID has been fixed.
37561	The Network Summary page in the WebUI now correctly shows mesh APs, even when mesh radios are disabled.
37785	SNMPv3 written details of System Contact, System Location, and System Name now correctly show up in both the CLI and WebUI.
38097	Native support for ZTE MF626 and Brazil Vivo carrier dialer group has been added to the 4306 Series switches.
38444	The range of valid addresses from a DHCP server, based on an entered range of excluded addresses, is no correctly displayed in the WebUI.
38603	Fpapps crash caused by a segmentation fault has been fixed.
38604, 38631	Fpapps crash caused by a segmentation fault has been fixed.
38786, 38780	The log message snmpGetCardTable has been removed from AOS-W.

Known Issues and Limitations in AOS-W 3.4.2.6

The following are known issues and limitations for this release of AOS-W. Applicable bug IDs or workarounds are included:

Table 9 *Known Issues and Limitations*

Bug ID	Description

42221	The following piece of information applies to customers having Chassis based switch (S-1, S-2 & S3) with a 24 port line Card (LC 1) placed in the upper slot.
	If you have VRRP instances (One or multiple) running between 2 or more such switches, please DO NOT execute the following commands on the switch with a BACKUP VRRP instance. These commands have been observed to cause VRRP to flap between the VRRP MASTER and the VRRP BACKUP when executed on the switch acting as the VRRP BACKUP.
	On the CLI:
	`#show poe`
	`#tar log tech-support`
	`#show tech-support`
	On the WebUI:
	Download logs with tech support

40032	The AP-105 frequently detects spurious radar on channels 52, 56, 60, and 64. This issue will affect connectivity on DFS channels.
39977	A kernal panic occurs regularly on the 651 when sending traffic to a wireless client.
39768	In 3.4.2.1, Kerberos configuration is only available in the CLI.
39620	In 3.4.2.1, users can delete the default-role which is being used in stateful Kerberos. This can lead to misconfiguration.
	In 3.4.2.1, Stateful Kerberos authentication currently does not work with NAT or PAT.
39426	An issue with walk/get of wlsxVoiceAPBssidInfoGroup causes multiple crashes in stm.
39256, 39370	STM on the master switch becomes busy if an L2 GRE tunnel connects the master to a local switch.
39072	When token-caching is enabled and a RADIUS server is used for authentication, the command `show user-table verbose` will incorrectly label the server as “Internal” instead of “RADIUS.”
38801	In the description for aaa password-policy mgmt password-max-character-repeat, the range is described as `Range: 0-10 special characters`. The range should read `Range: 0-10 characters/digits/special characters`.
38741	The maximum character length for `aaa password-policy mgmt password-min-length` is actually 32 characters, although it is stated to be 64 characters.
36507	When AP-105 is deployed as a Remote AP in bridge or split-tunnel mode, it is possible to observe an occasional AP kernel crash when the AP is submitted to a very large amount of UDP traffic. This is mostly a concern for throughput testing and is extremely unlikely to happen in any real usage scenario.
35349	The “Access Point Status” LED on a switch does not work unless rogue APs are detected.
35305	When disable scanning option is set for SIP ACLs, SIP packets are not reaching the ALG and hence ports are not being opened for RTP
35174	After an extended online session with the carrier, a cellular modem's communication port may become unresponsive and cause redial attempts to be unsuccessful. Unplug the USB data card and re-insert to remedy the problem.

Table 9 *Known Issues and Limitations (Continued)*

Bug ID	Description
35173	The VLAN map configuration is not propagated to a new local switch when it is configured on an existing master switch. Execute write memory on the master switch to remedy this issue.
34830	High re-associations are seen for Spectralink handsets connected to Mesh points.
34829	An error message is displayed when an OAW- AP60 is provisioned as mesh node.
34759	Do not manage or configure RFportect sensors using AOS-W 3.4. Doing so will cause unexpected switch behavior.
34615	4306 series switches freeze if the EVDO modem is plugged out while passing traffic through it
34408	4306 series switches may not behave normally if the RF-band is changed when the internal AP is in AM mode.
34103	PTT does not work on Spectralink phones when battery boost is enabled.
33898	Occasionally a Windows client prompts for a password to access the NAS disk although there is no password set for disk access. When this occurs, the user can access the NAS disk after closing the password prompt or by entering a random password.
32066	When the country code of a running AP is changed because its regulatory domain profile changed, the AP needs to be rebooted.
28983, 31509	Legacy APs operating on channels 52, 56, 60, and 64 often detect spurious radar while other APs, placed in same vicinity, do not.
20194	If Static WEP is used with split or bridge mode VAP’s, key slots 2-4 on the switch should be used. Key slot 1 should be used with VAP’s in tunnel mode only.

Documents in This Release

New revisions of the following documents are available with this release:

- *AOS-W 3.4.2 User Guide*
- *AOS-W 3.4.2 Command Line Interface Reference Guide*
- *AOS-W 3.4.2 Quick Start Guide*
- *AOS-W 3.4.2 MIB Reference Guide*
- *AOS-W 3.4.2 Software Upgrade Guide*

The documentation library is updated continuously. You can download the latest version of any of these documents from:

https://service.esd.alcatel-lucent.com

For More Information

To contact Alcatel-Lucent, refer to the information below:

Web Site Support	
Main Site	http://www.alcatel-lucent.com/enterprise
Support Site	https://service.esd.alcatel-lucent.com

Web Site Support	
Support Email	support@ind.alcatel.com

Telephone Numbers	
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe	+33 (0) 38 855 6929
Asia Pacific	+65 6240 8484

Alcatel·Lucent

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301